UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/811,585	03/29/2004	Jeffrey A. Aaron	BELL-0340/00379 C1	2073

39072 7590 10/22/2007
MYERS BIGEL SIBLEY & SAJOVEC, P.A.
P.O. BOX 37428
RALEIGH, NC 27627

EXAMINER	
PATEL, NIRAV B	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
10/22/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/811,585	AARON ET AL.	
	Examiner	Art Unit	
	Nirav Patel	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 August 2007 (Amendment)*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *29,31-35 and 43-52* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *29,31-35 and 43-52* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's amendment filed on Aug. 15, 2007 has been entered. Claims 29, 31-35, 43-52 are pending.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. Claims 45-52 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 45 recites "A computer program product *for monitoring* a networked computer system, the computer program *product comprising computer program code* embodied in a storage medium, *the computer program code comprising*: program code configured to sequentially poll a plurality of devices of the networked computer system for data relating to network communications thereof; program code configured to detect an anomaly responsive to polling of a first device in the computer system using network-based intrusion detection techniques comprising analyzing data entering into a plurality of hosts, servers, and computer sites in the networked computer system; and program code configured to determine a second device that is anticipated to be affected by the anomaly by using pattern correlations across the plurality of hosts, servers, and computer sites following the detection of the anomaly and prior to polling of the second device. The computer program product claim is merely stored so as to be

read or outputted by a computer **without creating any functional interrelationship, either as part of the stored data or as part of the computing processes performed by the computer**, then such descriptive material alone does not impart functionality either to the data as so structured, or to the computer. When nonfunctional descriptive material is recorded on some computer-readable medium, in a computer or on an electromagnetic carrier signal, it is not statutory since no requisite functionality is present to satisfy the practical application requirement. Therefore, claim 45 recites non-statutory subject matter.

Claims 46-52 depend on claim 45, therefore they are rejected with the same rationale applied against claim 45 above.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 29, 32, 33, 35, 43, 44, 45, 47, 48, 50-52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aucsmith et al (US Pub. No. 2003/0110392) and in view of Sheikh et al (US Pub. No. 2002/0078382).

As per claim 29, Aucsmith discloses:

detecting an anomaly at a first device in the computer system using network-based intrusion detection techniques comprising analyzing data entering into a plurality of hosts, servers and computer sites in the networked computer system [Fig. 1, paragraph 0037-0039, Fig. 2 step 206];

determining a second device that is anticipated to be affected by the anomaly by using pattern correlations across the plurality of hosts, servers, and computer sites following the detection of the anomaly and prior to polling of the second device (i.e. possible security problem) [Fig.1, paragraph 0043-0046, 0050, 0051, 0012, 0013].

Aucsmith teaches detecting an anomaly at a first device in the computer system [Fig. 1, paragraph 0039] and determining possible security intrusions/anomaly following the detection of the anomaly at the client [paragraph 0050,0051]. Aucsmith doesn't expressively mention polling a plurality of devices of the networked computer system.

Sheikh teaches:

polling a plurality of devices of the networked computer system in a predetermined sequential order for information relating to network communication thereof [Fig. 1, 1A, paragraph 0032 lines 5-9, 0042, Fig. 4].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Sheikh with Aucsmith, since one would have been motivated to monitor the computer network systems for security purposes [Sheikh, paragraph 003].

As per claim 32, the rejection of claim 29 is incorporated and Aucsmith teaches: the anomaly comprises one of an intrusion and an intrusion attempt [paragraph 0027 lines 7-17].

As per claim 33, the rejection of claim 29 is incorporated and Aucsmith teaches: analyzing a plurality of data packets with respect to predetermined patterns [Fig. 1, paragraph 0039].

As per claim 35, the rejection of claim 29 is incorporated and Aucsmith teaches: controlling the second device responsive to determining the second device is anticipated to be affected by the anomaly [paragraph 0012, 0013, Fig. 1].

As per claim 43, the rejection of claim 35 is incorporated and Aucsmith teaches: controlling a firewall of the second device responsive to determine the second device is anticipated to be affected by the anomaly [Fig. 1, paragraph 0054, 0057].

As per claim 44, the rejection of claim 35 is incorporated and Aucsmith teaches: Sending an alert to the second device prior to polling of the second device [Fig. 1, paragraph 0012, 0013, 0051].

As per claim 45, it encompasses limitations that are similar to limitations of claim 29. Thus, it is rejected with the same rationale applied against claim 29 above.

As per claim 47, the rejection of claim 45 is incorporated and it encompasses limitations that are similar to limitations of claim 32. Thus, it is rejected with the same rationale applied against claim 32 above.

As per claim 48, the rejection of claim 45 is incorporated and it encompasses limitations that are similar to limitations of claim 33. Thus, it is rejected with the same rationale applied against claim 33 above.

As per claim 50, the rejection of claim 45 is incorporated and it encompasses limitations that are similar to limitations of claim 35. Thus, it is rejected with the same rationale applied against claim 35 above.

As per claim 51, the rejection of claim 50 is incorporated and it encompasses limitations that are similar to limitations of claim 43. Thus, it is rejected with the same rationale applied against claim 43 above.

As per claim 52, the rejection of claim 45 is incorporated and it encompasses limitations that are similar to limitations of claim 44. Thus, it is rejected with the same rationale applied against claim 44 above.

4. Claims 31 and 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aucsmith et al (US Pub. No. 2003/0110392) in view of Sheikh et al (US Pub. No. 2002/0078382) and in view of Wolff et al. (US Pub. No. 2002/0174358).

As per claim 31, the rejection of claim 29 is incorporated and Aucsmith teaches that transmitting an anomaly warning from the first device to a central analysis engine, responsive to detecting the anomaly at the first device [Fig. 1, paragraph 0041 lines 1-5]. Aucsmith doesn't expressively mention that warning comprising a unique device identifier.

However, Wolff teaches that warning (i.e. report) comprising a unique device identifier [paragraph 0017 lines 1-4].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Wolff with Aucsmith and Sheikh, since one would have been motivated to obtain accurate picture of anomaly and to identify a particular event and a device [Wolff, paragraph 0005 lines 1-2, 0010 lines 1-2].

As per claim 46, the rejection of claim 45 is incorporated and it encompasses limitations that are similar to limitations of claim 31. Thus, it is rejected with the same rationale applied against claim 31 above.

5. Claim 34 and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aucsmith et al (US Pub. No. 2003/0110392) in view of Sheikh et al (US Pub. No. 2002/0078382) and in view of Wada et al (US Patent No. 7,047,142).

As per claim 34, the rejection of claim 33 is incorporated and Aucsmith teaches analyzing the received the data packet by the device [Fig. 1, paragraph 0025, 0039]. Wada teaches analyzing packets/data by at least two devices in the networked computer system [col. 2 lines 18-23].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Wada with Aucsmith and Sheikh, since one would have been motivated to monitor the various devices for predicting a/an failure/anomaly in the communication network [Wada, col. 1 lines 7-9].

As per claim 49, the rejection of claim 48 is incorporated and it encompasses limitations that are similar to limitations of claim 34. Thus, it is rejected with the same rationale applied against claim 34 above.

Response to Amendment

6. Applicant's arguments filed Aug. 15, 2007 have been fully considered but they are not persuasive.

Regarding to the Applicant's argument to the 35 USC § 101 rejections of claims 45-52, Examiner disagrees with applicant's remark and still maintains that claims 45-52 recite non-statutory matter. The claims limitations do not provide an explicit (inter) relationship between the computer/computer storage medium having computer executable instructions and a technological art, environment or machine that is required for the claims to be statutory. That is, the claimed limitation needs to explicitly show functional relationship between the stored executable instructions and a computer as part of the computing process performed by the computer.

Regarding to the applicant's argument to claims 29 and 45, Examiner maintains that the combination of Aucsmith and Sheikh teach the claim limitation "polling a plurality of devices of the networked computer system in a predetermined sequential order for information relating to network communications". Aucsmith teaches the network configuration as shown in Fig. 1. The client terminals (102(1) – 102(N)) each include an agent that monitor information received at its associated client terminal from the network. If one of the agents detects a possible security problem in any of the information, the agent reports the possible security problem to the server. The server propagates any possible security problems seen by any of the client terminals to all of the client terminals (also to the firewall) so that all of the client terminals defend against that possible security problem (prior to detecting at the other device/agent i.e. early or

possible anomaly). Further, Sheikh teaches a distributed data processing system as shown in Figs. 1, 1A. The network 100a comprises of a master transport located on a central server, which is dedicated to running the transport layer and storing results. The central server provides for polling of one or more agent transports, which are located throughout network on the agent transport's associated host servers. The agent transport implements sensor programs sequentially on the host server and actually performs the desired monitoring routines. The master transport connects to the agent transports in parallel as well as serially. The master transport polls the agent transports located on the host servers in the network to gather information from each agent transport. The sensor monitors all logs on the web servers, which serves as early warning system for possible attacks in the network. In this case, the combination of Aucsmith and Sheikh teaches the claim subject matter and the combination is sufficient to incorporate the teaching of Sheikh into the teaching of Aucsmith to poll a plurality of devices of the networked computer system in a predetermined sequential order for information relating to network communications and determine a second device that is anticipated to be affected by the anomaly following the detection of the anomaly and prior to polling of the second device (early or possible anomaly).

Further, Applicant argument regarding "timing relationship...", is not considered unless stated expressively in the claim language. The Applicant is reminded that additional modification to clarify the claimed language is necessary for further consideration and distinction from the prior art.

For the above reasons, it is believed that the rejections should be sustained.

Conclusion

7. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nirav Patel whose telephone number is 571-272-5936. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-273-8300. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

NBP
10/16/07

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100